UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/277,335	03/26/1999	DEAN A. KLEIN	MPATENT.053A	3400

20995	7590	04/20/2005	

KNOBBE MARTENS OLSON & BEAR LLP
2040 MAIN STREET
FOURTEENTH FLOOR
IRVINE, CA 92614

EXAMINER
PICH, PONNOREAY

ART UNIT	PAPER NUMBER
2135	

DATE MAILED: 04/20/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

-- *The MAILING DATE of this communication appears on the cover sheet with the correspondence address* --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>01 April 2005</u>.

2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-10 and 12-18</u> is/are pending in the application.

    4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) <u>1-10 and 12-18</u> is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

    a)☐ All   b)☐ Some *   c)☐ None of:

      1.☐ Certified copies of the priority documents have been received.

      2.☐ Certified copies of the priority documents have been received in Application No. _____.

      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
application from the International Bureau (PCT Rule 17.2(a)).

    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1)☒ Notice of References Cited (PTO-892)

2)☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3)☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
    Paper No(s)/Mail Date _____.

4)☒ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____.

5)☐ Notice of Informal Patent Application (PTO-152)

6)☐ Other: _____.

DETAILED ACTION

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 4/1/2005 has been entered.

The communication filed on 4/1/2005 amended claims 1, 5, 7, and 15. Claims 1-10 and 12-15 remain for examination.

The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

Response to Amendment

As indicated during the interview held on 3/29/2005, the applicant's amendments are enough to overcome the prior art used in the previous office action. However, new rejections are made below which include new art.

As per the amendments, the examiner would like to note that the applicant stated that the content of the configuration register is user defined in the specification (p8, lines 21-25). Also, a register is defined in the art as a storage device or storage location having a specified storage capacity. Therefore, the examiner asserts that the broadest reasonable interpretation of a configuration register is any storage device or storage location having a specified storage capacity.

Response to Arguments

Applicant's arguments with respect to claim 1-10 and 12-15 have been considered but are moot in view of the new ground(s) of rejection.

As per the arguments filed on 4/1/2005,   both the applicant and examiner agree that the prior art does not teach "retrieving a checksum from a configuration register in the personal computer and verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key." The examiner would like to note that the use of a checksum to verify a cryptographic key was admitted by the applicant as known to one of ordinary skill in the art at the time the applicant's invention was made (see specification, p10, lines 5-13). The examiner also notes that as the applicant discloses that using a checksum to verify a cryptographic key was known at the time the applicant's invention was made, motivation for verifying a cryptographic key and using a checksum to do so must also have existed in the art of cryptography during the time the applicant's invention was made.

The examiner notes that the applicant did not make any argument as to whether the prior arts used in the previous office action properly anticipated the set of claims as presented last time. Since the applicant filed an RCE and made no arguments, the examiner assumes that the applicant agrees that the prior arts were properly applied to the set of limitations addressed in the previous office action to show that the prior art do in fact anticipate the previous set of claims, which were the set prior to the current amendments. As such, the examiner references the previous office actions in their entirety and will only specifically address new limitations which were added by the amendments filed by the applicant on 4/1/2005.

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set
> forth in section 102 of this title, if the differences between the subject matter sought to be patented and
> the prior art are such that the subject matter as a whole would have been obvious at the time the
> invention was made to a person having ordinary skill in the art to which said subject matter pertains.
> Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3-6, and 17-18 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Olarig et al (US 6,032,257) and van Rumpt et al (US 5,513,262),

herein referred to as Rumpt1, in view of van Rumpt et al (US 5,231,662), herein referred

to as Rumpt2, and further in view of Easter et al (US 5,563,950).

Claim 1:

As per claim 1, a previous office action has addressed most of the limitations of

claim 1 already. As for the limitations that were not addressed in the previous office

action, they were amended onto claim 1 by the applicant and will now be addressed.

Olarig, Rumpt1, and Rumpt2 do not disclose:

1. Retrieving a checksum from a configuration register in the personal computer.

2. Verifying the generated cryptographic key, wherein verifying comprises

    determining a checksum of the generated key.

However, Easter discloses calculating a hash value for a cryptographic key and

storing the hash value (col 5, lines 32-35 and col 6, lines 23-25). Note that a checksum

is a hash value. Easter also discloses verifying a generated cryptographic key by

calculating the hash value of the key and then comparing the calculated hash value of

the key with the stored hash value (col 6, lines 23-34 and 48-50). The examiner asserts

that the place the first hash/checksum was stored reads on a configuration register.

Also, to compare the two hashes/checksums, the first hash/checksum value must be

obtained from the configuration register.

In light of the above teachings by Easter, it would have been obvious to one of

ordinary skill in the art at the time the applicant's invention was made to further modify

the combination method of Olarig, Rumpt1, and Rumpt2 according to the limitations

recited in claim 1. One of ordinary skill would have been motivated to do so as Easter

discloses that it is desirable to verify that a cryptographic key is good before it is used

(col 6, lines 28-34).

Claim 5:

As per claim 5, a previous office action has addressed most of the limitations of

claim 5 already. As for the limitations that were not addressed in the previous office

action, they were amended onto claim 5 by the applicant and will now be addressed.

Olarig, Rumpt1, and Rumpt2 do not disclose:

1. Providing a configuration for storing a checksum.

2. The encryption engine verifies the generated cryptographic key using the

   checksum.

However, as discussed in claim 1, Easter discloses calculating a hash value for a cryptographic key and storing the hash value (col 5, lines 32-35 and col 6, lines 23-25). Easter also discloses verifying a generated cryptographic key by calculating the hash value of the key and then comparing the calculated hash value of the key with the stored hash value (col 6, lines 23-34 and 48-50). The examiner asserts that the structure the hash value disclosed by Easter is stored is a configuration.

In light of the above teachings by Easter, it would have been obvious to one of ordinary skill in the art at the time the applicant's invention was made to further modify the combination method of Olarig, Rumpt1, and Rumpt2 according to the limitations recited in claim 5. One of ordinary skill would have been motivated to do so for the same reasons given in claim 1.

Claims 3-4, 6, and 17-18:

Olarig, Rumpt1, Rumpt2, and Easter disclose all the limitations of claim 1. In addition, Olarig discloses all the limitations 3 and 4 as indicated in a previous office action and claims 3 and 4 stand rejected. Further, claims 17 and 18 are identical to claims 3 and 4 respectively and are rejected on the same basis as claims 3 and 4 respecitvely.

Olarig and Rumpt1 disclose all the limitations of claim 6 as indicated in a previous office action.

Claims 13-14:

Olarig, Rumpt1, Rumpt2, and Easter disclose all the limitations of claim 1. In
addition, the rejection of claims 13-14 in view of Rumpt1 has been discussed in a
previous office action and the claims stand rejected.

Claims 2 and 16 are rejected under 35 U.S.C. 103(a) as being unpatentable over
Olarig et al (US 6,032,257) and van Rumpt et al (US 5,513,262), herein referred to as
Rumpt1, in view of van Rumpt et al (US 5,231,662), herein referred to as Rumpt2, and
further in view of Easter et al (US 5,563,950) and Hung et al (US 5,343,525).

Claim 2:

Olarig, Rumpt1, Rumpt2, and Easter disclose all the limitations of claim 1. In
addition, a previous office action discusses how Hung is applied in the rejection of claim
2. The rejection stands.

Claim 16:

Claim 16 is identical to claim 2 and is rejected for the same reasons.

Claims 7-10 and 12 are rejected under 35 U.S.C. 103(a) as being unpatentable
over Davis (US 5,818,939) in view of Olarig et al (US 6,032,257) and van Rumpt et al
(US 5,231,662), herein referred to as Rumpt2, and further in view of Easter et al (US
5,563,950).

Claim 7:

As per claim 7, a previous office action has addressed most of the limitations of

claim 7 already. As for the limitations that were not addressed in the previous office

action, they were amended onto claim 7 by the applicant and will now be addressed.

Davis, Olarig, and Rumpt2 do not disclose:

1. Retrieving a checksum from a configuration register in the computer system.

2. Verifying the generated cryptographic key, wherein verifying comprises

    determining a checksum of the generated key.

However, Easter discloses calculating a hash value for a cryptographic key and

storing the hash value (col 5, lines 32-35 and col 6, lines 23-25). Note that a checksum

is a hash value. Easter also discloses verifying a generated cryptographic key by

calculating the hash value of the key and then comparing the calculated hash value of

the key with the stored hash value (col 6, lines 23-34 and 48-50). The examiner asserts

that the place the first hash/checksum was stored reads on a configuration register.

Also, to compare the two hashes/checksums, the first hash/checksum value must be

obtained from the configuration register.

In light of the above teachings by Easter, it would have been obvious to one of

ordinary skill in the art at the time the applicant's invention was made to further modify

the combination system of Davis, Olarig, and Rumpt2 according to the limitations

recited in claim 7. One of ordinary skill would have been motivated to do so as Easter

discloses that it is desirable to verify that a cryptographic key is good before it is used (col 6, lines 28-34).

Claim 8:

Claim 8 contains all the limitations of claim 7. In addition, the limitations of claim 8 are disclosed by Davis as indicated in a previous office action.

Claim 9-10 and 12:

Claims 9 and 12 contain all the limitations of claim 7. In addition, the limitations of claims 9 and 12 are disclosed by Davis in view of Rumpt2 as indicated in a previous office action.

Claim 10 contains all the limitations of claim 9. In addition, the limitations of claim 10 are disclosed by Davis in view of Rumpt2 as indicated in a previous office action.

Claim 15:

As per claim 15, a previous office action has addressed most of the limitations of claim 15 already. As for the limitations that were not addressed in the previous office action, they were amended onto claim 15 by the applicant and will now be addressed.

Davis, Olarig, and Rumpt2 do not disclose:

1. Retrieving a checksum from a configuration register in the personal computer.

2. Verifying the generated cryptographic key, wherein verifying comprises determining a checksum of the generated key.

However, Easter discloses calculating a hash value for a cryptographic key and

storing the hash value (col 5, lines 32-35 and col 6, lines 23-25). Note that a checksum

is a hash value. Easter also discloses verifying a generated cryptographic key by

calculating the hash value of the key and then comparing the calculated hash value of

the key with the stored hash value (col 6, lines 23-34 and 48-50). The examiner asserts

that the place the first hash/checksum was stored reads on a configuration register.

Also, to compare the two hashes/checksums, the first hash/checksum value must be

obtained from the configuration register.

In light of the above teachings by Easter, it would have been obvious to one of

ordinary skill in the art at the time the applicant's invention was made to further modify

the combination method of Davis, Olarig, and Rumpt2 according to the limitations

recited in claim 15. One of ordinary skill would have been motivated to do so as Easter

discloses that it is desirable to verify that a cryptographic key is good before it is used

(col 6, lines 28-34).

Double Patenting

Applicant is advised that should claims 2, 3, and 4 be found allowable, claims 16,

17 and 18 will be objected to under 37 CFR 1.75 as being a substantial duplicate

thereof. When two claims in an application are duplicates or else are so close in

content that they both cover the same thing, despite a slight difference in wording, it is

proper after allowing one claim to object to the other as being a substantial duplicate of

the allowed claim. See MPEP § 706.03(k).

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Ponnoreay Pich whose telephone number is 571-272-7962. The examiner can normally be reached on 8:00am-4:30pm Mon-Fri.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on 571-272-3859. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

PP

SUPERVISOR PATENT EXAMINER
TECHNOLOGY CENTER 2100